

AMENDED IN SENATE MARCH 4, 2009

SENATE BILL

No. 20

Introduced by Senator Simitian

December 1, 2008

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 20, as amended, Simitian. Personal information: privacy.

Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the system or data, as defined, following discovery or notification of the security breach, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

This bill would require any agency, person, or business that must issue a security breach notification pursuant to existing law to fulfill certain additional requirements pertaining to the security breach notification, as specified.

The bill would also require any agency, person, or business that must issue a security breach notification to more than 500 California residents pursuant to existing law to electronically submit that security breach notification to the Attorney General.

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 1798.29 of the Civil Code is amended to read:

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that must issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information, ~~as defined in subdivision (g),~~ that were or are reasonably believed to have been the subject of a breach.

(C) The date, estimated date, or date range within which the breach occurred, if that information is possible to determine at the time the notice is provided, and the date of the notice.

1 (D) Whether the notification was delayed as a result of a law
2 enforcement investigation.

3 (E) A general description of the breach incident.

4 (F) The estimated number of persons affected by the breach.

5 (G) The toll-free telephone numbers and addresses of the major
6 credit reporting agencies if the breach exposed a bank account or
7 credit card number, a social security number, or a driver's license
8 or California identification card number.

9 (3) At the discretion of the agency, the security breach
10 notification may also include any of the following:

11 (A) Information about what the agency has done to protect
12 individuals whose information has been breached.

13 (B) Advice on steps that the person whose information has been
14 breached may take to protect himself or herself.

15 (e) Any agency that must issue a security breach notification
16 pursuant to this section to more than 500 California residents as a
17 result of a single breach of the security system shall electronically
18 submit that security breach notification to the Attorney General.

19 (f) For purposes of this section, "breach of the security of the
20 system" means unauthorized acquisition of computerized data that
21 compromises the security, confidentiality, or integrity of personal
22 information maintained by the agency. Good faith acquisition of
23 personal information by an employee or agent of the agency for
24 the purposes of the agency is not a breach of the security of the
25 system, provided that the personal information is not used or
26 subject to further unauthorized disclosure.

27 (g) For purposes of this section, "personal information" means
28 an individual's first name or first initial and last name in
29 combination with any one or more of the following data elements,
30 when either the name or the data elements are not encrypted:

31 (1) Social security number.

32 (2) Driver's license number or California Identification Card
33 number.

34 (3) Account number, credit or debit card number, in combination
35 with any required security code, access code, or password that
36 would permit access to an individual's financial account.

37 (4) Medical information.

38 (5) Health insurance information.

39 (h) (1) For purposes of this section, "personal information"
40 does not include publicly available information that is lawfully

1 made available to the general public from federal, state, or local
2 government records.

3 (2) For purposes of this section, “medical information” means
4 any information regarding an individual’s medical history, mental
5 or physical condition, or medical treatment or diagnosis by a health
6 care professional.

7 (3) For purposes of this section, “health insurance information”
8 means an individual’s health insurance policy number or subscriber
9 identification number, any unique identifier used by a health insurer
10 to identify the individual, or any information in an individual’s
11 application and claims history, including any appeals records.

12 (i) For purposes of this section, “notice” may be provided by
13 one of the following methods:

14 (1) Written notice.

15 (2) Electronic notice, if the notice provided is consistent with
16 the provisions regarding electronic records and signatures set forth
17 in Section 7001 of Title 15 of the United States Code.

18 (3) Substitute notice, if the agency demonstrates that the cost
19 of providing notice would exceed two hundred fifty thousand
20 dollars (\$250,000), or that the affected class of subject persons to
21 be notified exceeds 500,000, or the agency does not have sufficient
22 contact information. Substitute notice shall consist of all of the
23 following:

24 (A) E-mail notice when the agency has an e-mail address for
25 the subject persons.

26 (B) Conspicuous posting of the notice on the agency’s Web site
27 page, if the agency maintains one.

28 (C) Notification to major statewide media and the Office of
29 Information Security and Privacy Protection.

30 (j) Notwithstanding subdivision (i), an agency that maintains
31 its own notification procedures as part of an information security
32 policy for the treatment of personal information and is otherwise
33 consistent with the timing requirements of this part shall be deemed
34 to be in compliance with the notification requirements of this
35 section if it notifies subject persons in accordance with its policies
36 in the event of a breach of security of the system.

37 SEC. 2. Section 1798.82 of the Civil Code is amended to read:

38 1798.82. (a) Any person or business that conducts business
39 in California, and that owns or licenses computerized data that
40 includes personal information, shall disclose any breach of the

1 security of the system following discovery or notification of the
2 breach in the security of the data to any resident of California
3 whose unencrypted personal information was, or is reasonably
4 believed to have been, acquired by an unauthorized person. The
5 disclosure shall be made in the most expedient time possible and
6 without unreasonable delay, consistent with the legitimate needs
7 of law enforcement, as provided in subdivision (c), or any measures
8 necessary to determine the scope of the breach and restore the
9 reasonable integrity of the data system.

10 (b) Any person or business that maintains computerized data
11 that includes personal information that the person or business does
12 not own shall notify the owner or licensee of the information of
13 any breach of the security of the data immediately following
14 discovery, if the personal information was, or is reasonably
15 believed to have been, acquired by an unauthorized person.

16 (c) The notification required by this section may be delayed if
17 a law enforcement agency determines that the notification will
18 impede a criminal investigation. The notification required by this
19 section shall be made after the law enforcement agency determines
20 that it will not compromise the investigation.

21 (d) Any person or business that must issue a security breach
22 notification pursuant to this section shall meet all of the following
23 requirements:

24 (1) The security breach notification shall be written in plain
25 language.

26 (2) The security breach notification shall include, at a minimum,
27 the following information:

28 (A) The name and contact information of the reporting person
29 or business subject to this section.

30 (B) A list of the types of personal information, ~~as defined in~~
31 ~~subdivision (g)~~, that were or are reasonably believed to have been
32 the subject of a breach.

33 (C) The date, or estimated date, or date range within which the
34 breach occurred, if that information is possible to determine at the
35 time the notice is provided, and the date of the notice.

36 (D) Whether notification was delayed as a result of a law
37 enforcement investigation.

38 (E) A general description of the breach incident.

39 (F) The estimated number of persons affected by the breach.

1 (G) The toll-free telephone numbers and addresses of the major
2 credit reporting agencies if the breach exposed a bank account or
3 credit card number, a social security number, or a driver's license
4 or California identification card number.

5 (3) At the discretion of the person or business, the security
6 breach notification may also include any of the following:

7 (A) Information about what the person or business has done to
8 protect individuals whose information has been breached.

9 (B) Advice on steps that the person whose information has been
10 breached may take to protect himself or herself.

11 (e) Any person or business that must issue a security breach
12 notification pursuant to this section to more than 500 California
13 residents as a result of a single breach of the security system shall
14 electronically submit that security breach notification to the
15 Attorney General.

16 (f) For purposes of this section, "breach of the security of the
17 system" means unauthorized acquisition of computerized data that
18 compromises the security, confidentiality, or integrity of personal
19 information maintained by the person or business. Good faith
20 acquisition of personal information by an employee or agent of
21 the person or business for the purposes of the person or business
22 is not a breach of the security of the system, provided that the
23 personal information is not used or subject to further unauthorized
24 disclosure.

25 (g) For purposes of this section, "personal information" means
26 an individual's first name or first initial and last name in
27 combination with any one or more of the following data elements,
28 when either the name or the data elements are not encrypted:

29 (1) Social security number.

30 (2) Driver's license number or California Identification Card
31 number.

32 (3) Account number, credit or debit card number, in combination
33 with any required security code, access code, or password that
34 would permit access to an individual's financial account.

35 (4) Medical information.

36 (5) Health insurance information.

37 (h) (1) For purposes of this section, "personal information"
38 does not include publicly available information that is lawfully
39 made available to the general public from federal, state, or local
40 government records.

1 (2) For purposes of this section, “medical information” means
2 any information regarding an individual’s medical history, mental
3 or physical condition, or medical treatment or diagnosis by a health
4 care professional.

5 (3) For purposes of this section, “health insurance information”
6 means an individual’s health insurance policy number or subscriber
7 identification number, any unique identifier used by a health insurer
8 to identify the individual, or any information in an individual’s
9 application and claims history, including any appeals records.

10 (i) For purposes of this section, “notice” may be provided by
11 one of the following methods:

12 (1) Written notice.

13 (2) Electronic notice, if the notice provided is consistent with
14 the provisions regarding electronic records and signatures set forth
15 in Section 7001 of Title 15 of the United States Code.

16 (3) Substitute notice, if the person or business demonstrates that
17 the cost of providing notice would exceed two hundred fifty
18 thousand dollars (\$250,000), or that the affected class of subject
19 persons to be notified exceeds 500,000, or the person or business
20 does not have sufficient contact information. Substitute notice
21 shall consist of all of the following:

22 (A) E-mail notice when the person or business has an e-mail
23 address for the subject persons.

24 (B) Conspicuous posting of the notice on the Web site page of
25 the person or business, if the person or business maintains one.

26 (C) Notification to major statewide media and the Office of
27 Information Security and Privacy Protection.

28 (j) Notwithstanding subdivision (i), a person or business that
29 maintains its own notification procedures as part of an information
30 security policy for the treatment of personal information and is
31 otherwise consistent with the timing requirements of this part, shall
32 be deemed to be in compliance with the notification requirements
33 of this section if the person or business notifies subject persons in
34 accordance with its policies in the event of a breach of security of
35 the system.